

Teaching Case

Bank Solutions Disaster Recovery and Business Continuity: A Case Study for Business Students

Steve Camara

Senior Manager, KPMG LLP
1021 E Cary Street, Suite 2000
Richmond, VA 23219
scamara@kpmg.com

Robert Crossler

Vishal Midha

Assistant Professor
Computer Information Systems
The University of Texas – Pan American
recrossler@utpa.edu, vmidha@utpa.edu

Linda Wallace

Associate Professor
Accounting and Information Systems
Virginia Tech
wallacel@vt.edu

ABSTRACT

Disaster Recovery and Business Continuity (DR/BC) planning is an issue that students will likely come in contact with as they enter industry. Many different fields require this knowledge, whether employees are advising a company implementing a new DR/BC program, auditing a company's existing program, or implementing and/or serving as a key participant in a company program. Often times in the classroom it is difficult to find real world practice for students to apply the theories taught. The information in this case provides students with real world data to practice what they would do if they were on an engagement team evaluating a DR/BC plan. Providing students with this opportunity better prepares them for one of the jobs they could perform after graduation. This case gives students experience working at the individual level making decisions, at the dyadic level analyzing other people's decisions, and at the group level presenting an agreed upon analysis.

Keywords: Case study, Computer security, Critical thinking, Experiential learning & education, Information assurance and security, Role-play, Security, Team projects

1. CASE SUMMARY

This case is used by the authors during an information assurance course taught as part of an accounting and information systems degree. It is presented during the portion of the semester when business continuity and disaster recovery is being covered. The intent of the case is to give students an opportunity to gain real world experience with a

theoretical concept that can be difficult to comprehend fully. At the conclusion of this case, students should possess a greater understanding of the critical decision-making process that goes into analyzing and deciding what risks need to be dealt with as a part of a Disaster Recovery and Business Continuity (DR/BC) team.

This case is presented as a non-project based case (Cappel and Schwager 2002) and it is expected that students

will utilize higher level cognitive skills as presented in the classic taxonomy of Bloom (1956). They will accomplish this by distinguishing relevant from irrelevant facts, developing alternatives and solutions, and applying concepts to a specific situation.

To accomplish the stated goal of this case, information from a fictional company, Bank Solutions, Inc., is provided. Bank Solutions, Inc. is a provider of item processing services to community banks, savings and loan associations, Internet banks, and small- to mid-size credit unions. Bank Solutions, Inc. needs to identify its operating and regulatory risks. A professional business team is hired to identify the risks and provide recommendations to mitigate the identified risks.

2. CASE TEXT

2.1 Company Background

Bank Solutions, Inc. (a pseudonym), founded in 1973 by the First Presidential Bank, a major bank of its time, is a provider of item processing servicesⁱ to community banks, savings and loan associations, Internet banks, and small- to mid-size credit unions. It offers a full range of services, including inclearing and Proof of Deposit (POD) processing, item capture, return and exception item processing, image archive storage and retrieval, and customer statement rendering.

Bank Solutions was formed in 1973 when the Chief Operating Officer of First Presidential Bank, a major commercial bank, recognized an opportunity. Since item processing functions are standardized (they have to be in order for originating and receiving financial institutions to clear customer transactions) and scalable with increases in item processing volumes, they were able to offer these services to other financial institutions wishing to reduce operating expense and focus on growth strategies and other core business functions. First Presidential marketed these services under the Bank Solutions brand name.

Over the next 15 years, Bank Solutions enjoyed modest growth. By 1988, it served 41 small- to mid-size financial institutions. It had not, however, developed a market presence outside of the Northwestern Region of the United States, as management had hoped. This was primarily because Bank Solutions was unable to compete with other item-processing service providers that had developed proprietary software systems considered “top of the line.” To make matters worse, at the time almost one quarter of Bank Solutions’ client base was saving and loan associations (saving and loans). As a result of the Savings and Loan crisis, 60% of Bank Solutions’ savings and loan customer base failed over the six years spanning 1985–1991, thus stunting the outsourcer’s growth. The related slow down of the financial services and real estate industries and the recession of 1990–1991 presented further headwinds to the growth objectives of First Presidential management. In 1994, First Presidential sold off Bank Solutions.

Under new management, Bank Solutions thrived. Keys to the company’s renewed success included the following:

- The development of key strategic partnerships with other industry participants, including data clearing houses and financial institution core processing system outsourcers.ⁱⁱ

- The introduction of a new company culture that focused on open door management, mentoring, and enhanced employee benefits.
- The development of a proprietary, state of the art item processing system that uses state-of-the-art Optical Character Recognition (OCR) technology to achieve character recognition accuracies that were previously unheard of.
- The implementation of “remote capture” technologiesⁱⁱⁱ to meet electronic banking initiatives and regulations such as “Check 21.”
- The upgrade or replacement of other administrative information systems, including the company’s financial reporting system. This helped to increase operational effectiveness and efficiencies.

From 1995–2008, Bank Solutions enjoyed unprecedented growth. During that timeframe, the company expanded operations to 18 item processing facilities, two data centers in which the item processing system was hosted, and 345 financial institutions.

2.2 Current Scenario (2011)

Douglas Smith, the Chief Information Officer for Bank Solutions, was one of the original members of “new management” and responsible for many of Bank Solutions’ past successes. A solid, middle-sized company with continued growth potential, Bank Solutions has become a target for a leveraged corporate buyout. This is an attractive situation for Douglas and other members of executive management. Several of these individuals are close to retirement; and initial indications are that the price of the buyout will be very favorable for members of executive management.

The CEO and other influential members of executive management want Bank Solutions to remain an attractive purchase option and, as a result, have contracted the services of your team as an outside consultant to identify operating and regulatory risks and advise them on control measures to mitigate the risks.

2.3 Risk Assessment Task

As members of the engagement team performing the risk assessment, your team has been given the task of assessing Bank Solutions’ incident handling, business continuity, and disaster recovery strategy.

In order to perform the assessment, preliminary interviews with Douglas Smith, the Data Center Managers, Systems Engineers and Network Architect in each of Banking Solutions’ data centers, and the IT Managers and Day and Night Operations Managers from seven of the largest item processing facilities were conducted. Additionally, the following documentation related to Bank Solutions’ security incident management, DR/BC planning activities was reviewed:

- Flow charts that diagram the item processing operations and data flow between Bank Solutions item processing facilities and data centers and outside entities (see Appendix A)
- A diagram of Bank Solutions’ network architecture

- Bank Solutions' Data Center Disaster Recovery and Business Continuity Plan (DRBCP)
- Policies, procedures, guidelines, and standards related to security incident response
- Item Processing Facility DRBCPs
- Results from the most recently completed DRBCP test/exercise
- Distribution list for the DRBCP
- Bank Solutions' Backup and Recovery Policy.
- Screen prints of the configurations from Bank Solutions' backup utility (these configurations show what server shares are subject to automated backup and the frequency of those backups)
- Contracts with the off-site storage provider
- A system-generated listing of access to event logging servers
- A list of individuals who have been provided access to recall backup tapes from the off-site storage vendor.
- Screenshots of the Intrusion Detection System (IDS), firewall, and other event logging capability configurations
- Excerpts from the IDS and firewall event logs and management's manually maintained incident tracking log.

2.4 Facts: Risk Assessment Findings

Based on the discussions held with the management and a review of the documentation provided, you note the following facts:

1. With the assistance of an external consultant, Bank Solutions wrote its current data center DRBCP in 2007. It was last updated in January 2009.
2. According to Douglas, the data center DRBCP was last tested in 2007. Testing activities consisted of a conceptual, table-top walkthrough of the DRBCP conducted by Douglas with the Data Center Managers and Network and Systems Engineers. Item processing facility DRBCPs have not yet been tested.
3. Site-specific DRBCPs have been written for the five largest item processing facilities. The remaining item processing facilities have a generic "small center" DRBCP template that was distributed to and customized by facility management in June 2010. Four item processing facilities have not yet completed the customization exercise.
4. DRBCPs contain several sections, including the following:
 - Emergency/crisis response procedures
 - Business recovery procedures
 - "Return to normal" procedures
 - Various appendices

Recovery Time Objectives and Recovery Point Objectives^{iv} for each critical business process and system were not identified in the DRBCP. The following details, most of which are included in the DRBCP appendices, are also documented in the text of the DRBCP:

- Critical systems, including detailed hardware and software inventories
 - Critical business processes and process owners
 - Alternative processing facility addresses and directions
 - "Calling Trees" (notification listings)
 - Critical plan participant roles, responsibilities, and requirements
 - Critical vendor contact listings
 - Key business forms
 - Specific recovery procedures for key systems
 - Procedures for managing public relations and communications
5. Based on a review of DRBCP distribution lists, it appears that not all key plan participants have a copy of the plan. When this was discussed with Douglas, he responded that copies of all DRBCPs are stored on the network (which is replicated across both data centers and via backup tape).
 6. Critical plan participants have not been trained to use DRBCPs.
 7. Bank Solutions has implemented a robust host-based IDS, including detailed event logging and reporting capabilities. However, neither the DRBCP nor any other policy, standard, guideline, or procedure addresses security incident handling steps, including escalation points of contact and procedures for preserving the forensic qualities of logical evidence.
 8. Event logging is also performed when power users perform specific privileged activities on production servers and selected administrative back office systems. Interestingly, it was noted that several of the same power users whose actions are recorded onto event logs also have write access to the logs themselves.
 9. A review of the network diagram and conversations with the Network Architect reveal that redundancies have been implemented at the network perimeter (e.g., routers, firewalls, IDS, load balancers, etc.).
 10. Banking Solutions has organized their DR/BC program according to a "sister center" format; that is, each data center serves as the other's "hot site" processing location and each item processing facility has been assigned a corresponding item processing facility to serve as a backup processing location. Neither the DRBCPs nor any other documentation outline specific processing responsibilities for backup facilities.
 11. On a daily basis, transaction detail and item image files from the current day's processing operations are uploaded from each item processing facility to their regional data center (see Appendix A).
 12. At the data centers, electronic vaulting has been established whereby all e-mail, file, and application servers and databases at the data center are continuously backed up to the other data center via dual dedicated fiber optic lines.
 13. A data backup and recovery utility has been implemented in each data center and the item processing facilities. Full backups of critical data files, software programs, and configurations are performed

once a week and incremental backups are performed on a daily basis Monday through Friday.

14. At one item processing facility, backup jobs have routinely failed due to unknown causes. When the topic was discussed with the IT Manager on duty, he shrugged the failures off noting that the core financial institution transaction data and images are transmitted to and archived at the Bank Solutions Data Center East on a daily basis.
15. At the item processing facilities, the management has been tasked with contracting the off-site storage of backup tapes. At one of the item processing facilities, management has contracted the bank across the street to store its backup tapes in a safety deposit box. At another item processing facility, the night Operations Manager stores the backup tapes in a safe at his home. At a third item processing center, tapes are stored in a shed at the back of the building.

3. EXERCISES AND SUBMISSIONS¹

This is a group project and each group should ideally consist of six students. Each group of students will work as a member of an engagement team in charge of performing the incident handling, DR/BC risk assessment for Bank Solutions. Each group should read the case background and the facts identified in the interviews.

Individual Work: For *all* of the facts/ findings, prepare a written report that lists the condition(s) that present risks to Bank Solutions as well as proposed recommendations for addressing those conditions. All the individual reports **MUST** have the individual's name on it.

Dyadic Work: Exchange your report with another student in your group. At this time, you will have the other students report with you. Read that report carefully, and further refine your list being sure that you agree to the conditions, risks, and recommendations that are mentioned in the other students' individual report. All the dyadic work **MUST** have names of both individuals.

Group Work: Together as a group, prepare a report of recommendations for correcting each of the aforementioned conditions (thereby addressing the risks) from the *assigned subset of facts*. Prepare to discuss your results in class. You should be ready to explain and elaborate on why you identified each condition and each risk. You will have about five minutes to present your subset of conditions, risks, and recommendations.

To Submit:

1. Six individual reports
2. Six dyadic reports
3. One group report

Subsets of Facts to be Analyzed

| Subset # | Fact #s |
|----------|---------|
| 1 | 1-3 |
| 2 | 4-5 |
| 3 | 6-8 |

| | |
|---|-------|
| 4 | 9-10 |
| 5 | 11-13 |
| 6 | 14-15 |

4. ENDNOTES

ⁱ Item processing operations play a critical role in financial institutions' ability to receive, record, and process customer transactions in an accurate, reliable, and timely manner. The item processing function converts data from hardcopy source documents including checks and customer transaction tickets (also known as 'items'), into an electronic format the institution's systems can capture and use in an automated environment. It is a function institutions can do internally or outsource [as in the case of Bank Solutions], in a centralized or decentralized manner. (Source: Federal Financial Institutions Examination Council Operations Handbook, Appendix C – Item Processing, July 2004)

ⁱⁱ Core processors are internally (with financial institutions) and externally (outsourced) organized entities that administer, support, and operate financial institution transaction processing systems. These systems are complex computer programs designed to process various types of financial institution transactions and serve as the financial institutions' general ledgers. Once transactions are sent and posted to core processor transaction systems, they are said to have been "cleared."

ⁱⁱⁱ Remote capture refers to the capture of electronic check images that are transmitted to the item processing facility. The item processing facility receives the files, formats and edits them, merges them with data files created from the receipt and processing of hardcopy items, and sends the resulting combined file to the appropriate core processor for clearing. Remote capture reduces the expense associated with management of hardcopy items, including the transport, sorting, imaging, and storage costs, as well as the time taken to clear items. Remote capture comes in two flavors – merchant capture and branch capture. Merchant capture is when a merchant (e.g., Wal-Mart, Best Buy, etc.) scans a check at the point of sale (POS) and the imaged check is sent in batch at specified closing times during the day directly to the item processor. These batches are edited and balanced, and the totals are sent to the core processor for clearing. Branch capture is similar, except that electronic capture is performed at banks where they scan the checks and other customer transaction documents and forward the files to item processing facilities for editing, balancing, and processing.

^{iv} Recovery Time Objective is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity (source: Wikipedia; Web address: http://en.wikipedia.org/wiki/Recovery_Time_Objective). Recovery Point Objective describes the amount of data lost measured in time. Example: If the last available good copy of data upon an outage was from 18 hours ago, then the RPO would be 18

¹ Please see Teaching Notes for explanation.

hours (source: Wikipedia; Web site: http://en.wikipedia.org/wiki/Recovery_point_objective).

5. REFERENCES

- Bloom, Benjamin S., (1956) "Cognitive Domain," *Taxonomy of Educational Objectives. Handbook 1*. New York: David McKay.
- Cappel, James J., and Schwager, Paul H. (2002) "Writing IS teaching cases: Guidelines for JISE submission," *Journal of Information Systems Education* Vol. 13, No. 4, pp. 287–293.

AUTHOR BIOGRAPHIES

Stephen L. Camara is a senior manager in KPMG LLP's Federal Information Technology Advisory Services practice in the Richmond, Virginia office. He performed/ managed Statement on Auditing Standards (SAS) No. 70 and Statement on Standards for Attestation Engagements (SSAE) No. 16 examinations for a variety of Federal and commercial clients and industries in the United States, Europe and Asia. Mr. Camara managed application, platform, and function-based information technology (IT) control assessments in the United States and Europe. Mr. Camara performed/managed IT internal control testing supporting Federal and commercial financial statement audits and audits performed in accordance with Sarbanes-Oxley (SOX) Section 404.



Robert Crossler is an Assistant Professor in the Computer Information Systems department at The University of Texas – Pan American. His research focuses on the factors that affect the security and privacy decisions that individuals make. He has several publications in the IS field, including such outlets as *MIS Quarterly*, the *Journal of Information Systems Security*, *Americas Conference on Information Systems*, and *Hawaii International Conference on System Sciences*. He also serves on the editorial review board for the *Journal of Organizational and End User Computing*, the *Information Resources Management Journal*, and the *Journal of Information Systems Security*. Prior to his academic career he worked as a database programmer, where he led many projects to completion and coordinated the work of others.



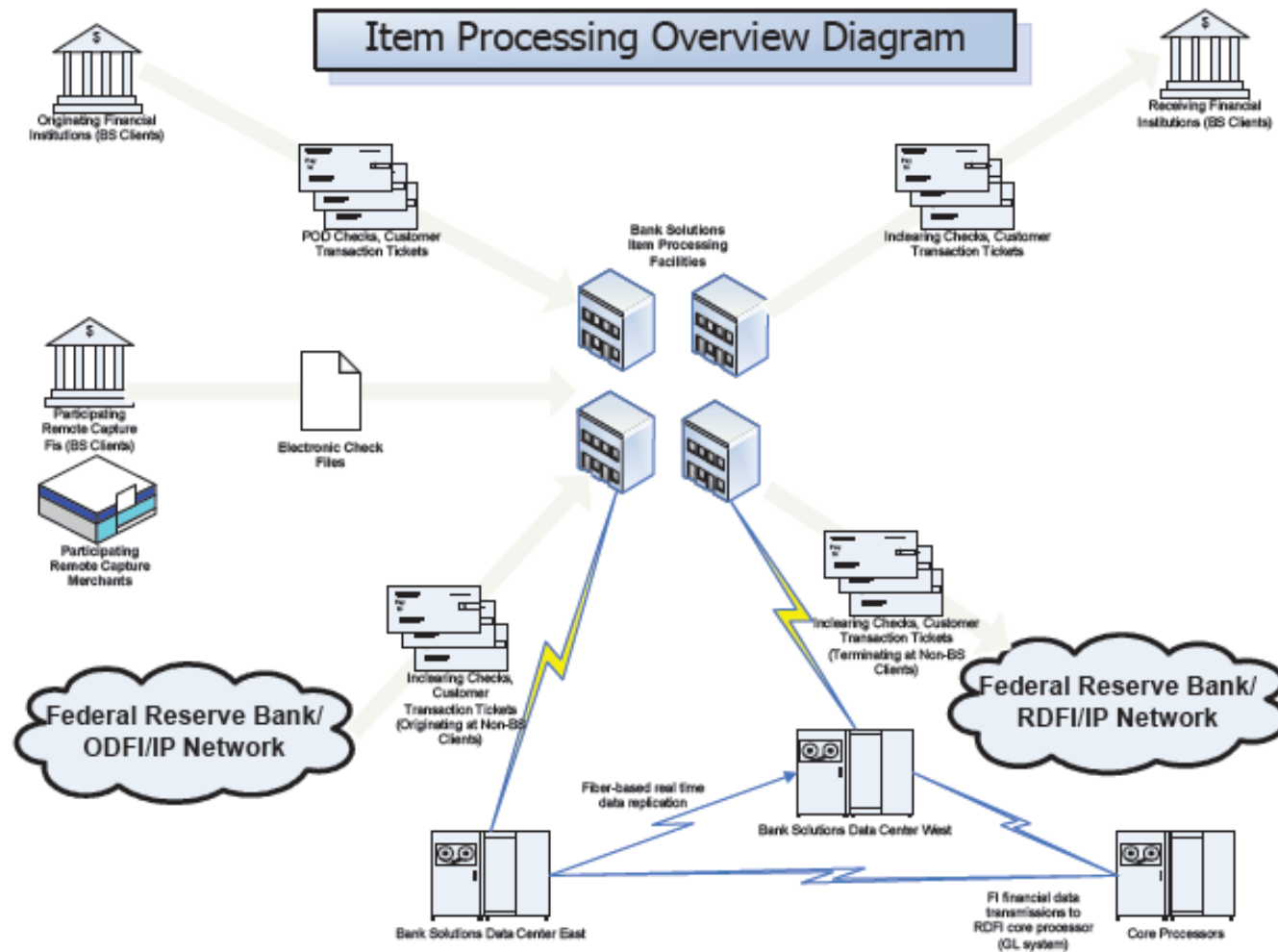
Vishal Midha is an assistant professor of Computer Information Systems at the University of Texas-Pan American. He has a Ph.D. in Information Systems from the University of North Carolina at Greensboro. His current other research interests include open source software development, information piracy concerns, and knowledge management. He has published in

Communications of AIS, *Electronic Markets*, *Journal of CIS*, and many national and international conferences including *ICIS*, *AMCIS*, *DSI*, and *GITMA*. Presently, he also serves as an Associate Editor for *Case Studies in International Journal of Information Security and Privacy*.

Linda Wallace is an associate professor in the Department of Accounting and Information Systems at Virginia Tech. Her research interests include software project risk, information security, knowledge communities, and agile software development. Her research has been accepted for publication in *Decision Sciences*, *Communications of the ACM*, *Information & Management*, *IEEE Security & Privacy*, *Decision Support Systems*, *Journal of Systems and Software*, and the *Journal of Information Systems*.



Appendix A



This case was developed solely for class discussion. While the situation described in this case is based on realistic events, the Bank Solutions is a fictional organization. Further, the names, product/service offerings, and the names of all individuals in the case are fictional. Any resemblance to actual companies, offerings, or individuals is accidental.



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

Copyright ©2011 by the Information Systems & Computing Academic Professionals, Inc. (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to the Editor-in-Chief, Journal of Information Systems Education, editor@jise.org.

ISSN 1055-3096